

Serial No. **10/061,363**
Amdt. dated May 5, 2008
Reply to Office Action of February 5, 2008

Docket No. **CIT/K-0137**

REMARKS/ARGUMENTS

Claims 1-16, 18-19, and 22-28 are pending. By this Amendment, claims 1, 5, 7, 11, 14, and 19 are amended, claims 17, 20, and 21 are canceled without prejudice or disclaimer, and claims 22-28 are added. No new matter is added. Support for the claims can be found throughout the specification, including the original claims, and the drawings. Reconsideration in view of the above amendments and following remarks is respectfully requested.

The Office Action rejected claims 1, 5, 9-11, 13-14, and 16-17 as being unpatentable over Sims III, U.S. Patent No. 6,550,011, in view of Ho, U.S. Patent No. 6,148,342, and further in view of Van Oorshot, U.S. Patent No. 6,229,894, and Czajkowski, U.S. Patent No. 7,100,048. Claim 17 has been canceled. The rejection is respectfully traversed in so far as it applies to the pending claims.

The Office Action asserts that Sims III teaches all of the claimed features of independent claims 1, 5, 11, and 14 except that "Sims III fails to teach sending private key identification by encrypting an ID," and that "Sims III fails to teach a master key or encrypting said master key with device[s] public key." The Examiner then asserts that Ho teaches "encrypting an identifier using a public key of the recipient (media certificate), (col. 3, lines 54-56)," and "finding the corresponding private key to decrypt the identifier, (col. 3, lines 57-59)." The Examiner then concludes that "[i]t would have been obvious to one of ordinary skill in the art to use the identifier of Ho with the DRM of Sims III because it allows the recipient to find the private key

Serial No. **10/061,363**
Amndt. dated May 5, 2008
Reply to Office Action of February 5, 2008

Docket No. **CIT/K-0137**

needed to decrypt future submissions from the sender.” The Examiner further asserts that “Van Oorshot teaches updating the public key certificate using a new public and private key (col. 6, line 64 –col. 7, line 4),” and concludes that “[i]t would have been obvious to one of ordinary skill in the art to update the certificate on a periodic basis in order to prevent key compromise.”

Additionally, the Examiner asserts that “Czajkowski teaches a method upon which a master key (private key, Figure 4, 48) is encrypted with the device[s] public key (public key, Figure 4, 50),” and further that “Czajkowski teaches encrypting that data with said master key, and the receiver decrypting the master key with the device[s] public key, and decrypting the message with the master key (private key) (Figure 4, col. 4, lines 10-37, col. 5, lines 10-15).” The Examiner then concludes that “[i]t would have been obvious to one of ordinary skill in the art to use the key of Czajkowski with the previous system because it allows additional security protection.”

The Examiner asserted that Czajkowski teaches a “master” key pair. That is, the Examiner interpreted that the private key 48 (= sender’s private key 60) as corresponding to the claimed master private key of independent claim 1, 5, 11, and 14. However, it is respectfully submitted that the sender’s private key 48, 60 corresponds to the claimed media key of independent claims 1, 5, 11, and 14, and that the receiver’s private and public keys correspond to the claimed private and public keys of a playing device. See col. 4, lines 31-34 and col. 5, lines 11-14 of Czajkowski. Thus, the sender’s private key 48, 60 does not correspond to the claimed

Serial No. **10/061,363**

Docket No. **CIT/K-0137**

Amdt. dated May 5, 2008

Reply to Office Action of February 5, 2008

master private key of independent claims 1, 5, 11, and 14. As previously submitted, in the claimed features, the playing device contains a master key pair as well as the media key transmitted by a sender and the private key of the playing device.

Further, it is respectfully submitted that the Examiner's piecemeal rejection of the independent claims 1, 5, 11, and 14 using four separate references is clearly based on improper hindsight gleaned from Applicants' own disclosure.

Accordingly, the rejection of independent claims 1, 5, 11, and 14 over Sims III, Ho, Van Oorshot, and Czajkowski should be withdrawn. Dependent claims 9-10, 13, 16, and 18, as well as added claims 22-28, are allowable over Sims III, Ho, Van Oorshot, and Czajkowski at least for the reasons discussed above with respect to independent claims 1, 5, 11, and 14, from which they respectively depend, as well as for their added features.

The Office Action rejected claims 2-4, 6-8, 12, and 15 under 35 U.S.C. §103(a) as being unpatentable over Sims III in view of Ho and Van Oorshot, and further in view of Czajkowski and Zubeldia, U.S. Patent No. 6,044,462. The rejection is respectfully traversed.

Dependent claims 2-4, 6-8, 12, and 15 are allowable over Sims III, Ho, Van Oorshot, and Czajkowski at least for the reasons discussed above with respect to independent claims 1, 5, 11, and 14, from which they respectively depend, as well as for their added features. Zubeldia fails to overcome the deficiencies of Sims III, Ho, Van Oorshot, and Czajkowski, as it is merely cited

Serial No. **10/061,363**

Docket No. **CIT/K-0137**

Amdt. dated May 5, 2008

Reply to Office Action of February 5, 2008

for allegedly teaching a key list with revoked keys. Accordingly, the rejection should be withdrawn.

CONCLUSION

In view of the foregoing amendments and remarks, it is respectfully submitted that the application is in condition for allowance. Favorable consideration and prompt allowance are earnestly solicited.

If the Examiner believes that any additional changes would place the application in better condition for allowance, the Examiner is invited to contact the undersigned attorney at the telephone number listed below.

Serial No. **10/061,363**

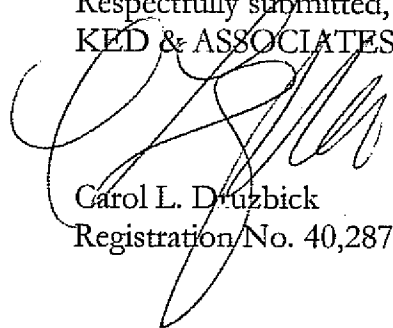
Docket No. **CIT/K-0137**

Amdt. dated May 5, 2008

Reply to Office Action of February 5, 2008

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this, concurrent and future replies, including extension of time fees, to Deposit Account 16-0607 and please credit any excess fees to such deposit account.

Respectfully submitted,
KED & ASSOCIATES, LLP



Carol L. Druzbeck
Registration No. 40,287

P.O. Box 221200

Chantilly, Virginia 20153-1200

(703) 766-3777 CLD:tlg

Date: May 5, 2008

\\Fk4\Documents\2016\2016-249\158314.doc

Please direct all correspondence to Customer Number 34610